Вестник Донского государственного технического университета. 2018. Т. 18, № 3. С. 333–338. ISSN 1992-5980 eISSN 1992-6006
Vestnik of Don State Technical University. 2018. Vol. 18, no. 3, pp. 333–338. ISSN 1992-5980 eISSN 1992-6006

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT



УДК 00.004 https://doi.org/10.23947/1992-5980-2018-18-3-333-338

Выбор элементов комплекса защиты информационной системы предприятия на основе требований нормативно-правовых документов[*]

Е. А. Витенбург[1], А. А. Левцова[2]**
[1, 2] Волгоградский государственный университет, г. Волгоград, Российская Федерация

Selecting safety package components of enterprise information system following requirements of standard legal documents[***]

E. A. Vitenburg [1], A. A. Levtsova [2]**
[1, 2] Volgograd State University, Volgograd, Russian Federation

Введение. Качество производственных процессов во многом зависит от инфраструктуры управления — в частности, от эффективности информационной системы (ИС). Менеджмент компаний уделяет все большее внимание обеспечению безопасности этой сферы, на ее поддержку регулярно направляются финансовые, материальные и другие ресурсы. В представленной работе рассмотрены вопросы построения комплекса защиты информационной системы предприятия.
Материалы и методы. Охрана ИС предприятия учитывает особенности объекта защиты и актуальные угрозы информационной безопасности. В рамках данного исследования принято, что ИС представляет собой комплекс информационных ресурсов. По результатам специального анализа определены категории угроз информационной безопасности предприятия: взлом; утечка; искажение; утрата; блокирование; злоупотребление. Выявлена связь данных угроз, компонентов ИС и элементов комплекса защиты. Рассмотрены требования нормативно-правовых актов Российской Федерации и международных стандартов, регулирующих данную сферу. Показано, каким образом результаты данного анализа позволяют обосновать выбор элементов комплекса защиты ИС.
Результаты исследования. Сравнительный анализ регламентирующей литературы, относящейся к данному вопросу, позволил выявить следующее. Разные документы предлагают разный набор элементов (подсистем) комплекса защиты ИС предприятия. Разрабатывая программу защиты ИС, следует руководствоваться Приказом ФСТЭК № 239 и стандартом 800-82 Revision 2 Guide to ICS Security.
Обсуждение и заключения. Результаты представленного исследования являются основой для формирования программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии. В частности, можно разрабатывать гибкие комплексы, позволяющие расширять состав элементов (подсистем).

Introduction. Production processes quality depends largely on the management infrastructure, in particular, on the information system (IS) effectiveness. Company management pays increasingly greater attention to the safety protection of this sphere. Financial, material and other resources are regularly channeled to its support. In the presented paper, some issues on the development of a safety enterprise information system are considered.
Materials and Methods. Protection of the enterprise IS considers some specific aspects of the object, and immediate threats to IT security. Within the framework of this study, it is accepted that IS are a complex of data resources. A special analysis is resulted in determining categories of threats to the enterprise information security: hacking; leakage; distortion; loss; blocking; abuse. The connection of these threats, IS components and elements of the protection system is identified. The requirements of normative legal acts of the Russian Federation and international standards regulating this sphere are considered. It is shown how the analysis results enable to validate the selection of the elements of the IS protection system.
Research Results. A comparative analysis of the regulatory literature pertinent to this issue highlights the following. Different documents offer a different set of elements (subsystems) of the enterprise IS protection system. To develop an IS protection program, you should be guided by the FSTEC Order No. 239 and 800-82 Revision 2 Guide to ICS Security.
Discussion and Conclusions. The presented research results are the basis for the formation of the software package of intellectual support for decision-making under designing an enterprise information security system. In particular, it is possible to develop flexible systems that allow expanding the composition of the components (subsystems).



[*] Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации в рамках НИР «Построение модели интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии».
[**] E-mail: e.vitenburg@ec-rs.ru, alexandra.levtsova@yandex.ru
[***] The research is done with the financial support from the Russian Federation President Council on Grants within the frame of R&D “Building a model of intellectual support for decision-making when designing an enterprise information security system”.

Ключевые слова: информационная система, информационная безопасность, система защиты информации, подсистемы защиты информации.

Keywords: information system, information security, information security system, information security subsystems.

Образец для цитирования: Витенбург, Е. А. Выбор элементов комплекса защиты информационной системы предприятия на основе требований нормативно-правовых документов / Е. А. Витенбург, А. А. Левцова // Вестник Дон. гос. техн. ун-та. — 2018. — Т. 18, № 3. — С. 333−338. https://doi.org/10.23947/1992-5980-2018-18-3-333-338

For citation: E.A. Vitenburg , A.A. Levtsova. Selecting safety package components of enterprise information system following requirements of standard legal documents. Vestnik of DSTU, 2018, vol. 18, no.3, pp. 333−338. https://doi.org/10.23947/1992-5980-2018-18-3-333-338

Введение. Информационные системы (ИС) все активнее используются в производственных и управленческих процессах. В связи с этим обостряется проблема информационной безопасности (ИБ) ИС. В частности, недостаточная изолированность ИС упрощает несанкционированный доступ к ним [1, 2, 3]. Последствиями вредоносного воздействия на ИС могут быть простои производства, финансовые потери, а при реализации худшего сценария — даже техногенные катастрофы [4]. Таким образом, актуальной задачей является формирование комплекса защиты промышленных ИС, эффективно препятствующего злоумышленным действиям.

Материалы и методы. Создание комплекса защиты информации основывается на результатах предпроектного обследования, в ходе которого определяются состав объекта защиты и актуальные для него угрозы.

Объект защиты представляется как множество информационных ресурсов:

$$Object_{Sec} = \{NE, CC, IS, Sts, WS, PE, OS, SS, AS, IP, Sn, RSM, SM, IA\}.$$

Здесь NE — множество сетевого оборудования; CC — множество каналов связи; IS — множество инфраструктурных серверов; Sts — множество систем хранения данных; WS — множество рабочих станций пользователей; PE — множество периферийного оборудования; OS — множество операционных систем; SS — множество системного программного обеспечения (ПО); AS — множество прикладного ПО; IP — множество информационных процессов, протекающих в ИС предприятия; Sn — подсети; RSM — множество съемных носителей информации; SM — электронные носители информации; IA — информационные активы.

Множество актуальных угроз ИБ $Threat$ определяется [5]:

$$Threat = \{Breaking, Leak, Distortion, Loss, Blocking, Abuse\}.$$

Здесь $Breaking$ — угрозы взлома; $Leak$ — угрозы утечки информации; $Distortion$ — угрозы искажения; $Loss$ — угрозы утраты; $Blocking$ — угрозы блокирования информационных ресурсов ИС предприятия; $Abuse$ — угрозы злоупотреблений.

Комплекс, противодействующий данным угрозам, представляет собой систему защиты ИС предприятия (СЗИС) (рис. 1).

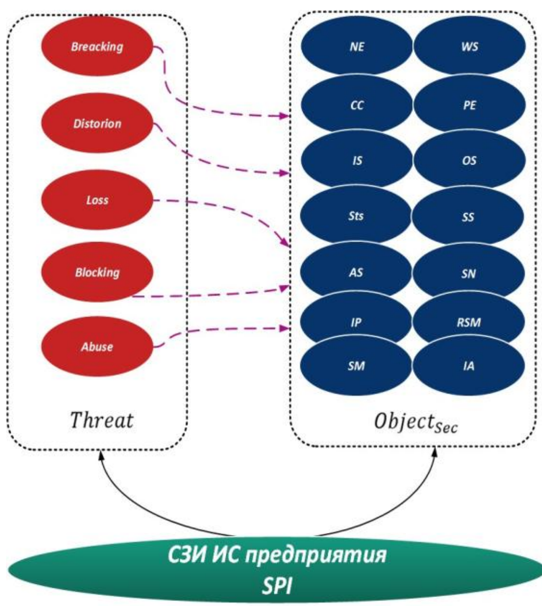


Рис. 1. Взаимосвязь объектов защиты и угроз в схеме СЗИС

Система защиты информации SPI (*system of protection of information*) — двухуровневая и включает подсистемы (компоненты) [6]:

— множество подсистемы ($Subsystem$)защиты информации;
— множество средств защиты (MP, *means of protection*) информации.

В общем виде структура СЗИС представлена на рис. 2.

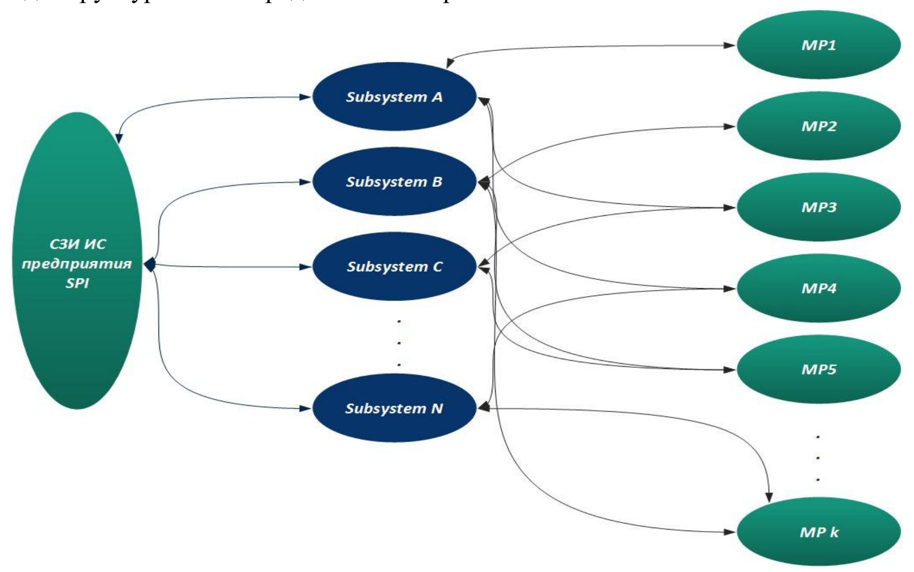


Рис. 2. Обобщенная структура СЗИС предприятия

При определении компонентов комплекса защиты информации специалисты исходят из анализа имеющейся нормативно-правовой документации и стандартов, действующих на предприятии. Необходимо также учитывать международный опыт. Довольно широко в мировой и отечественной практике применяется стандарт 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security [1]. Он разработан Национальным институтом стандартов и технологий США. В нем, в частности содержатся рекомендации по повышению безопасности в системах промышленного контроля, включая системы диспетчерского управления и сбора данных. Показано, каким угрозам подвергаются организационные процессы и бизнес-функции, описаны типичные уязвимости. Особое внимание уделяется мерам безопасности и контрдействиям, которые следует предпринять в угрожающей ситуации.

Результаты исследования. Отечественные нормативно-правовые акты (НПА), регламентирующие вопросы защиты ИС предприятия, условно можно разделить на две категории [6]:
— НПА по обеспечению информационной безопасности автоматизированных систем управления технологическим процессом (АСУ ТП);
— НПА по защите критической информационной инфраструктуры (КИИ).

Следует особо отметить, что уязвимости в защите КИИ могут повлечь значительный материальный и экологический ущерб. Недостаточная охрана КИИ чревата социальными и военно-политическими проблемами.

Проектирование системы защиты информации (в частности, при создании модели интеллектуальной поддержки принятия решений) предполагает предварительное проведение сравнительного анализа профильных нормативно-правовых актов Российской Федерации. Следует рассмотреть, например, следующие документы:
— Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [7];
— Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов информационной инфраструктуры Российской Федерации» (проект) [8];
— международный стандарт 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security [9].

Сравнительный анализ Приказов ФСТЭК России № 31 и № 239 представлен в табл. 1.

Таблица 1

Элементы (подсистемы) комплекса защиты ИС предприятия в Приказах ФСТЭК России № 31 и № 239

Подсистемы СЗИС	Приказ ФСТЭК от 14.03.14 № 31	Приказ ФСТЭК от 25.12 2017 г. № 239
	Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
	Управление доступом субъектов доступа и объектов доступа (УПД)	
	Ограничение программной среды (ОПС)	
	Защита машинных носителей информации (ЗНИ)	
	Регистрация событий безопасности (РСБ)	Аудит безопасности (АУД)
	Антивирусная защита (АВЗ)	
	Обнаружение вторжений (ОВ)	Предотвращение вторжений (ПВ)
	Контроль (анализ) защищенности информации (АНЗ)	Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
	Обеспечение целостности (ОЦЛ)	
	Обеспечение доступности (ОДТ)	
	Планирование мероприятий по обеспечению защиты информации (ПЛН)	
	Защита технических средств и систем (ЗТС)	
	Обеспечение безопасности разработки программного обеспечения (ОБР)	Реагирование на инциденты информационной безопасности (ИНЦ)
	Защита среды виртуализации (ЗСВ)	Информирование и обучение персонала (ИПО)
	Управление обновлениями программного обеспечения (ОПО)	
	Обеспечение действий в нештатных ситуациях (ДНС)	
	Анализ угроз безопасности информации и рисков от их реализации (УБИ)	—
	Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)	
Примечание. Для большей наглядности отличия не только разнесены по разным ячейкам, но и выделены серым фоном.		

Итак, Приказ ФСТЭК № 239 предусматривает наличие в комплексе защиты ИС предприятия следующих подсистем:

— аудит безопасности (АУД);

— защита информационной (автоматизированной) системы и ее компонентов (ЗИС);

— реагирование на инциденты информационной безопасности (ИНЦ);

— информирование и обучение персонала (ИПО).

Следует отметить, что решение о комплектности СЗИС до известной степени зависит от финансовых возможностей предприятия. Однако если стоимость защищаемых ресурсов и потенциальный ущерб от злоумышленных действий выше, чем стоимость СЗИС, то целесообразно внедрить АУД и ЗИС.

Сравнительный анализ Приказа ФСТЭК от 25 декабря 2017 г. № 239 и стандарта 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security приведен в табл. 2.

Таблица 2

Элементы (подсистемы) комплекса защиты ИС предприятия в Приказе ФСТЭК от 25 декабря 2017 г. № 239 и стандарте 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security)

Подсистемы СЗИС	Приказ ФСТЭК от 25.12 2017 г. № 239	800-82 Revision 2 Guide to ICS Security
	Идентификация и аутентификация (ИАФ) Identification and authentication	
	Управление доступом (УПД) System and communications protection, Security assessment and authorization	
	Ограничение программной среды (ОПС)	System and information integrity
	Защита машинных носителей информации (ЗНИ) Media protection	
	Аудит безопасности (АУД) Auditing and accountability	
	Антивирусная защита (АВЗ)	System and information integrity

П о	Приказ ФСТЭК от 25.12 2017 г. № 239	800-82 Revision 2 Guide to ICS Security
	Предотвращение вторжений (компьютерных атак) (СОВ)	System and information integrity
	Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	System and information integrity
	Обеспечение целостности (ОЦЛ)	System and information integrity
	Обеспечение доступности (ОДТ) System and services acquisition	
	Планирование мероприятий по обеспечению безопасности (ПЛН) Planning, contingency planning	
	Защита технических средств и систем (ЗТС) Maintenance	
	Реагирование на инциденты информационной безопасности (ИНЦ) Incident response	
	Информирование и обучение персонала (ИПО) Personnel security	
	Управление обновлениями программного обеспечения (ОПО)	Organization — wide information security program management controls
	Обеспечение действий в нештатных ситуациях (ДНС) Physical and environmental protection Awareness and training	
	Управление конфигурацией (УКФ) Configuration management	
	—	Risk assessment
	—	System and communications protection
Примечание. Для большей наглядности отличия не только разнесены по разным ячейкам, но и выделены серым фоном.		

В данном случае наиболее очевидны следующие различия:

— 800-82 Revision 2 Guide to ICS Security объединяет в подсистеме System and information integrity функционал подсистем ОПС, АВЗ, СОВ, ОЦЛ, ЗИС, определенных в Приказе ФСТЭК;

— 800-82 Revision 2 Guide to ICS Security предусматривает наличие подсистемы защиты систем связи — System and communications protection;

— Приказ ФСТЭК объединяет в подсистеме управления доступом (УПД) функционалы подсистем System and communications protection и Security assessment and authorization;

— Приказ ФСТЭК объединяет в подсистеме планирования мероприятий по обеспечению безопасности (ПЛН) функционал подсистем Planning и Contingency planning;

— Приказ ФСТЭК объединяет в подсистеме обеспечения действий в нештатных ситуациях (ДНС) функционал подсистем Physical and environmental protection и Awareness and training.

Следует особо указать на подсистемы оценки рисков и защиты систем связи [10]. Это наиболее важные элементы комплекса защиты ИС предприятия, из тех, которые не предусмотрены отечественной нормативно-правовой документацией. Их внедрение позволит усилить защиту, оперативно реагировать на инциденты, возникающие в ИС предприятия, своевременно и точно противодействовать атакам.

Выводы. Результаты анализа элементов комплекса защиты ИС будут использованы для построения модели интеллектуальной поддержки принятия решений при проектировании СЗИС. В частности, планируется предусмотреть возможность расширения состава подсистем СЗИС. Выбор элементов такого комплекса будет зависеть от оценки рисков, размера потенциального ущерба от вредоносного воздействия, стоимости компонентов СЗИС.

Библиографический список

1. Ovsyanitskaya, L. Yu. Information security of small business: modern Condition, problems and the ways of their Solutions / L. Yu. Ovsyanitskaya, Yu. V. Podpovetnaya, A. D. Podpovetnyy // Вестник Южно-Уральского гос. ун-та. — 2017. — № 4. — С. 77–84. — (Компьютерные технологии, управление, радиоэлектроника).

2. Glukhov, V. V. Problems of data protection in industrial corporations enterprise architecture / V. V. Glukhov, I. V. Ilin, A. B. Anisiforov // SIN'15 : Proceedings of the 8th International Conference on Security of Information and Networks. — New York : ACM, 2015. — P. 34–37.

3. Пищик, Б. Н. Безопасность АСУ ТП [Электронный ресурс] / Б. Н. Пищик // Вычислительные технологии. — 2013. — Т. 18, спецвыпуск. — С. 170–175. — Режим доступа: http://www.ict.nsc.ru/jct/t18n7 (дата обращения: 22.07.18).

4. Безопасность промышленных систем в цифрах [Электронный ресурс] / Г. Грицай [и др.]. — Москва : Positive Technologies, 2012. — 37 с. — Режим доступа: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (дата обращения: 22.07.18).

5. Мукминов, В. А. Методика оценки реального уровня защищенности автоматизированных систем / В. А. Мукминов, В. М. Хуцишвили, А. В. Лобузько // Программные продукты и системы. — 2012. — № 1 (97). — С. 39–42.

6. Лукацкий, А. Обзор мировых стандартов ИБ АСУ ТП и советы по их применимости в российских условиях [Электронный ресурс] / А. Лукацкий // Cisco Systems : Docplayer. — Режим доступа http://docplayer.ru/33122677-Obzor-mirovyh-standartov-ib-asu-tp-i-sovety-po-ih-primenimosti-v-rossiyskih-usloviyah.html (дата обращения: 22.07.18).

7. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 [Электронный ресурс] / Федеральная служба по техническому и экспортному контролю. — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 22.07.18).

8. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 [Электронный ресурс] / Федеральная служба по техническому и экспортному контролю. — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/1593-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 22.07.18).

9. Guide to Industrial Control Systems (ICS) Security / K. Stouffer [et al.] ; U. S. Department of Commerce ; National Institute of Standards and Technology. — Gaithersburg : NIST, 2015. — 247 p.

10. Singhal, A. Security risk analysis of enterprise networks using probabilistic attack graphs / A. Singhal, X. Ou // Network Security Metrics. — Cham : Springer, 2017. — P. 53–73.

Поступила в редакцию 21.06 .2018
Сдана в редакцию 25.06.2018
Запланирована в номер 20.07.2018

Received 21.06 .2018
Submitted 25.06.2018
Scheduled in the issue 20.07.2018

Об авторах:

Витенбург Екатерина Александровна,
аспирант кафедры «Информационная безопасность» Волгоградского государственного университета (РФ, 400062, г. Волгоград, пр. Университетский,100),
ORCID: https://orcid.org/0000-0002-1534-8865
e.vitenburg@ec-rs.ru

Левцова Александра Александровна,
студент кафедры «Информационная безопасность» Волгоградского государственного университета (РФ, 400062, г. Волгоград, пр. Университетский, 100),
ORCID: https://orcid.org/0000-0002-4798-9704
alexandra.levtsova@yandex.ru

Authors:

Vitenburg, Ekaterina A.,
postgraduate student of the Information Security Department, Volgograd State University (100, Universitetskiy pr., Volgograd, 400062, RF),
ORCID: https://orcid.org/0000-0002-1534-8865
e.vitenburg@ec-rs.ru

Levtsova, Alexandra A.,
student of the Information Security Department, Volgograd State University (100, Universitetskiy pr., Volgograd, 400062, RF),
ORCID: https://orcid.org/0000-0002-4798-9704
alexandra.levtsova@yandex.ru